

PTO/SB/08a/b (07-05)

Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1935, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Subs	titute for form 1449A/B/F	PTO			Complete if Known
				Application Number	10/081,863-Conf. #2605
IN	FORMATIO	N DISC	LOSURE	Filing Date	February 20, 2002
S	TATEMENT	BY AP	PLICANT	First Named Inventor	C. Andrew Neff
				Art Unit	2134
	(Use as many sheets as necessary)		Examiner Name	T. Tran	
Sheet	1	of	1	Attorney Docket Number	324628006US3

			U.S. PA	TENT DOCUMENTS	
Examiner Initials*	Cite No.1	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
とい		US-20020077885-A1	06-20-2002	Karro et al.	
ELT		US-6,540,138-B2	04-01-2003	Hall et al.	

	· · · · · · · · · · · · · · · · · · ·	FOREI	GN PATENT	DOCUMENTS		
Examiner Ci	Cite	Foreign Patent Document	Publication	Name of Patentee or	Pages, Columns, Lines,	
Initials*	No.1	Country Code ³ -Number ⁴ -Kind Code ³ (if known)	Date MM-OD-YYYY	Applicant of Cited Document	Where Relevant Passages or Relevant Figures Appear	
ELL		JP-10-257047	09-25-1998	Oki Electric Ind. Co. Ltd.		_
ELT				Nippon Telegr. & Teleph. Corp.		

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. *CITE NO.: Those application(s) which are marked with an single asterisk (*) next to the Cite No. are not supplied (under 37 CFR 1.98(a)(2)(iii)) because that application was filed after June 30, 2003 or is available in the IFW. ¹ Applicant's unique citation designation number (optional). ² See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. ³ Enter Office that Issued the document, by the two-letter code (WIPO Standard ST.3). ⁴ For Japanese patent documents, the Indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here If English language Yranslation is attached.

		NON PATENT LITERATURE DOCUMENTS	
Examiner Initials	Cite No.1	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
Fit		SCHNEIER, Bruce, "Applied Cryptography, Second Edition," John Wiley & Sons, Inc., 1996, pages 476-481, 490-491, and 532-533	
ELT		Davies, D. W., et al., "Security for Computer Networks," John Wiley & Sons, Ltd., Great Britain, 1984, pp. 253-257	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 809. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

'Applicant's unique citation designation number (optional). ³Applicant is to place a check mark here if English language Translation is attached.

	*************	***************************************		
Examiner I	×O n	Λ	Date	
Signature	(P	7	12	1100,00
Olgrisitire			Considered	10000

PTO/SB/08a/b (07-05)

Approved for use through 07/31/2006. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

TRADE TO THE Paperwork Reduction Act of 1995, no persons are required to respond to a collection of Information unless it contains a valid OMB control number.

Sut	estitute for form 1449A/B/PT	0		Complete if Known		
				Application Number	10/081,863-Conf. #2605	
11	NFORMATION	1 DI	SCLOSURE	Filing Date	February 20, 2002	
S	TATEMENT I	BY /	APPLICANT	First Named Inventor	C. A. Neff	
				Art Unit	2134	
	(Use as many sh	eets as	necessary)	Examiner Name	T. Tran	
Sheet	. 1	of	1	Attorney Docket Number	324628006US3	

	U.S. PATENT DOCUMENTS						
Examiner Initials*	Cite No.1	Document Number Number-Kind Code ² (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear		

	,	FOREIG	GN PATENT	DOCUMENTS	······································	-			
Examiner	Cite	Foreign Patent Document	Publication	Name of Patentee or	Pages, Columns, Lines,				
initials*	No.				Country Code ³ -Number ⁴ -Kind Code ⁵ (if known)	Date MM-DD-YYYY	Applicant of Cited Document	Where Relevant Passages or Relevant Figures Appear	T
ECT		JP-08-263575	10-11-1996	NEC Corp.					
4		JP-08-315053	11-29-1996	NEC Corp.					

^{*}EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. Applicant's unique citation designation number (optional). See Kinds Codes of USPTO Patent Documents at www.usprio.gov or MPEP 901.04. Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁵ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁶ Applicant is to place a check mark here if English language

		NON PATENT LITERATURE DOCUMENTS	
Examiner Initials	Cite No.¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T²
ECT		Benaloh, J. et al., "Receipt-Free Secret-Ballot Elections," Proceedings of 26th ACM Symposium on Theory of computing, Montreal, May 1994, pp. 544-553	
-1	-	Chaum, D., "Secret-Ballot Receipts: True Voter-Verifiable Elections," IEEE Computer Society, IEEE Security & Privacy, January-February 2004, Vol. 2, No. 1, pp. 38-47	
		Chaum, D., et al., "Wallet Databases with Observers," CRYPTO, 1992, Vol. 740, Lecture Notes in Computer Science, pp. 89-105	
		Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", European Transactions on Telecommunications, September-October, 1997, pp 481-490, 8(5), EUREL Publication, 1997	
		Koblitz, N., "Public Key," Chapter IV, A Course in Number Theory and Cryptograph, 2 nd Edition, pp. 83-124, Springer-Verlag, 1994	
		Naor, M., et al., "Visual Cryptograph," Eurocrypt 94, LNCS, Springer-Verlag, Berlin, 1995, Vol. 950, pp. 1-12	
		Neff, C.A., "A Verifiable Secret Shuffles and its Application to E-Voting," Eighth ACM Conference on Computer and Communications Security (CCS-8), November 2001, pp. 116-125	

^{&#}x27;EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Oraw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

^{&#}x27;Applicant's unique citation designation number (optional). 'Applicant is to place a check mark here if English language Translation is attached.

Examiner 1	l Date	1
Signature 5 7	Date	1 1 人がいたなく!
Signature C	/ IConsidered	1 100000

	SIPE	`
		NFORMATION DISCLOSURE STATEMENT BY APPLICANT
	DET. 0 6 200	Form PTO-1449 (Modified)
(A)	Bre musical	Use several sheets if necessary)

	COMPLETE IF KNOWN	_
Application Number	10/081,863	
Confirmation Number	2605	
Filing Date	February 20, 2002	
First Named Inventor	C. Andrew Neff	
Group Art Unit	2134	
Examiner Name	Gregory Allan Morse	
Attorney Docket No.	324628006US3	

					U.S. PATENT DOCUMENTS			
Examiner Initials	Cite No.			plication Kind Code (if known)	Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Line Where Relevant Figures Appear	s,
ELT		6,76	59,613	B2	McDermott et al.	8/3/04		
	_	_	······································					
		+						
		-						
		-						
		-	· · · · · · · · · · · · · · · · · · ·					
								·····
	······			F	OREIGN PATENT DOCUMENT			
Examiner Initial	Cite No.	Fore Office	eign Patent or A	Application Kind Cod (if know		Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Figures Appear	т
:								-
								+-
								+-
								-
			<u> </u>					
			OTHER	PRIOR	ART-NON PATENT LITERATUR or (in CAPITAL LETTERS), title of the a	RE DOCUMENTS	title of the item	7
Examiner Iritials	Cite No.	(b	ook, magazine	, journal, ser	ial, symposium, catalog, etc.), date, pag and/or country where publis	ge(s), volume issue numb	er(s), publisher, city	т

EXAMINER	er L	DATE CONSIDERED
*EXAMINER:	Initial if reference considered, whether or not criteria is in confort considered. Include copy of this form with next communication to	nance with MPEP 609. Draw line through citation if not in conformance and not
	considered. Include copy of this form with next communication t	o application(s).

PEZ	`,				COMPLETE IF KNOWN
)	^`; ►		•	Application Number	10/081,863
JAH 20 2004	UNFORMATION	DISCLOSURE		Confirmation Number	2605
JAH C	STATEMENT E	BY APPLICANT		Filing Date	February 20, 2002
ري ريخ	Form PTO-14 (Use several she	149 (Modified)	_	First Named Inventor	C. Andrew Neff
CAT & TRANS	(Use several she	ets if necessary)	Group Art Unit	2132
				Examiner Name	Gilberto Barron, Jr.
Sheet	1	of	1	Attorney Docket No.	324628006US3

				Ĺ	.S. PATENT DOCUMENTS			
Examiner Initials	Cite No.	:		ation d Code known)	Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	s,
								,,,,,,
							ECEIVED	
							JAN 2,7 2004	
						Tecl	mology Center 210	0
•	+							
•		- I		FOF	REIGN PATENT DOCUMENTS	S .		
Examiner	Cite No.	Fore	eign Patent or App	lication Kind Code (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Figures Appear	T
ECT	710.	CA	2,176,990		Kilian et al.	11/20/96		-
								-
Examiner Initials	Cite No.	(b	Include name o	f the author	T-NON PATENT LITERATUR (in CAPITAL LETTERS), title of the ar symposium, catalog, etc.), date, page and/or country where publish	ticle (when appropriate) e(s), volume issue numb		7
				 				

EXAMINER	20	In.	DATE CONSIDERED
*EXAMINER:	Initial if reference considered, whether or not cri considered. Include copy of this form with next		nance with MPEP 609. Draw line through citation if not in conformance and not o application(s).

PTO/SB/08a/b (08-03) \
Approved for use through 07/31/2006, OMB 0651-0031
U.S. Paters and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Sub	ostilute for form 1449A/B/PT	0	· · · · · · · · · · · · · · · · · · ·	Complete If Known		
				Application Number	10/081,863-Conf. #2605	
11	NFORMATION	I DI	SCLOSURE	Filing Date	February 20, 2002	
S	STATEMENT BY APPLICANT			First Named Inventor	C. A. Neff	
	·			Art Unit	2134	
	(Use as many sh	eets as	necessary)	Examiner Name	Gregory Allan Morse	
Sheet	heet 1 of 1		Altomey Docket Number	324628006US3		

	U.S. PATENT DOCUMENTS										
Examiner Initials*	Cite No. 1	Document Number Number-Kind Code ² (If known)	Publication Date MM-DD-YYYY	I Italia or rateixes of	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear						
Ec C		US-6,021,200	02-01-2000	Fischer, Jean-Bernard							
V		US-6,550,675	04-22-2003	Davis et al.							

		FOREIG	GN PATENT I	DOCUMENTS		
Examiner Initials*	Cite No. 1	Foreign Patent Document Country Code ³ -Number ⁴ -Kind Code ⁵ (il known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T
						Г

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with rext communication to applicant. "Applicants urique citation designation number (optional). "See Kinds Codes of USPTO Patent Documents at www.usptp.gov.or/MPEP-901.04. "Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). "For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. "Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible." Applicant is to place a check mark here if English language Translation is attached.

		NON PATENT LITERATURE DOCUMENTS	
Examiner Initials	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T²
	,		

EX-MINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

RECEIVED

AUG 1 8 2004

Technology Center 2100

	42			
Examiner	P 12	1	Date	
Signature	1 +	la a cita	Considered	1 2000
(3		700	001344400	

¹Applicant's unique citation designation number (optional). 2Applicant is to place a check mark here if English language Translation is attached.

	OIPE					COMPLIE IF KNOWN
	~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~ ~				Application Number	10/081,863
/ ,	W	INFORMATION		•	Confirmation Number	2605
- M	MAY 2 0.2004 STATEMENT BY APPLICANT				Filing Date	February 20, 2002
PATER	ج چ	Form PTO-14	•		First Named Inventor	C. Andrew Neff
100	MADEMARY	(Use several she	ets if necessary))	Group Art Unit	2134
	WYDEM.			····	Examiner Name	Gregory Allan Morse
l	Sheet	1	of	1	Attorney Docket No.	324628006US3

		***************************************			U.S. PATENT DOCUMENT	rs	
Examiner Initials			. Kind Code Name of Patentee or Inventor		Date of Publication or Filing Date or of Cited Document	Pages, Columns, Lines, Where Relevant Figures Appear	
ECT		6,09	92,051		Kilian et al.	7/18/00	
						RE	CEIVED
						M	AY 2-4 2004
					· · · · · · · · · · · · · · · · · · ·	Techno	logy Center 2100
					· · · · · · · · · · · · · · · · · · ·		
		 		F	OREIGN PATENT DOCUME	NTS	
Examiner Initial	Cite No.	Fore Office	eign Patent or A	pplication Kind Coo (if know		Date of Publication or Filing Date cant of Cited Document	Pages, Columns, Lines, Where Relevant Figures Appear T
			OTHER	PRIOR A	ART-NON PATENT LITERAT	URE DOCUMENTS	
Examiner Initials	Cite No.	(b	Include name	of the auth	or (in CAPITAL LETTERS), title of ti ial, symposium, catalog, etc.), date, and/or country where pu	he article (when appropriate) page(s), volume issue numb	, title of the item per(s), publisher, city

EXAMINER .	Ĉ (2	DATE CONSIDERED
*EXAMINER:	Initial if reference considered, whether	er or not criteria is in conforr	nance with MPEP 609. Draw line through citation if not in conformance and not
	considered. Include copy of this form	n with next communication t	o application(s).

COMPLETE IF KNOWN STATEMENT BY APPLICANT Form PTO-1449 (Modified) 10/081,863 Application Number Confirmation Number 2605 Filing Date February 20, 2002 Form PTO-1449 (Modified) First Named Inventor C. Andrew Neff (Use several sheets if necessary) Group Art Unit 2132 Examiner Name Gilberto Barron, Jr. Sheet 1 of Attorney Docket No. 324628006US3

				U.S. PATENT DOCUMENTS						
Examiner Initials	Cite No.			Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Line Where Relevant Figures Appear	es,			
FCT		4,774,665		Webb	9/27/88					
		5,610,383		Chumbley	3/11/97					
		5,875,432		Sehr	2/23/99	DECEN				
	6,250,548 B1		McClure et al.	6/26/01	RECEIVE					
V	6,317,833 B		B1	Jakobsson	11/13/01	JUN 3 0 2	003			
						Technology Cent	ter 2 10			
					·					
			F	OREIGN PATENT DOCUMENTS						
Examiner Initial			Kind Co		Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Figures Appear	Т			
·	-						+-			
							+			
							+			
		OTH	ER PRIOR A	ART-NON PATENT LITERATURI	E DOCUMENTS	I				
Examiner Initials	Cite No.	include na	me of the auth	or (in CAPITAL LETTERS), title of the art fal, symposium, catalog, etc.), date, page and/or country where publishe	ticle (when appropriate)	, title of the item per(s), publisher, city	Ţ			
ECT		International I PCT/US01/43		y Examination Report, Inter		tion No.				

EX \MINER	Et h	DATE CONSIDERED
*EXAMINER:	Initial if reference considered, whether or not criteria is in conformation to considered. Include copy of this form with next communication to	nance with MPEP 609. Draw line through citation if not in conformance and not
	considered. Include copy of this form with next communication t	o application(s).

To Fresh)			COMPLETE IF KNOWN				
φ	رِينَ مارين	. 5:00: 60:15=		Application Number	10/081,863			
MON 1 5 3005	STATEMENT E	DISCLOSURE		Confirmation Number	2605			
Kur	ATENIENIE			Filing Date	February 20, 2002			
PATENT & TEACH	Form PTO-14	149 (Modified)		First Named Inventor	C. Andrew Neff			
ENT 8 TEND	(Use several she	ets if necessary)	Group Art Unit	2132			
,				Examiner Name	Unknown			
Sheet	11	of	1	Attorney Docket No.	324628006US3			

					U.S. PATENT DOCUMENTS							
Examiner Initials	Cit No	e	S. Patent or Applicati Kind (BER (if kn		Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines Where Relevant Figures Appear	ş.				
ECT.		6,08	81,793		Challener et al.	6/27/00						
						+ RE	CEIVED					
						1 3 2002						
\ <u></u>					Tachnolo	- 0 2002						
						1001111010	y Center 2100					
· · · · · · · · · · · · · · · · · · ·	-							\dashv				
	SORION DATENT DOGUMENTS											
	FOREIGN PATENT DOCUMENTS Date of Date of											
Examiner Initial	Cite No.	Office	Ki	nd Code	The state of the s	Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Figures Appear					
ECT		PCT	WO92/03805	A1	Tecnomen Oy	3/5/92	<u> </u>	T				
FCT		PCT	WO01/22200	A2	VoteHere, Inc.	3/29/01						
								\Box				
	<u> </u>	<u> </u>	OTHER PR	OR AF	RT-NON PATENT LITERATURE I	DOCUMENTS		버				
Examiner Initials	Cite No.	(b	Include name of thook, magazine, journ	e author al, seria	(in CAPITAL LETTERS), title of the articl I, symposium, catalog, etc.), date, page(s) and/or country where published.	, volume issue numb	, title of the item per(s), publisher, city	T				
E(1					Voting, Computerized polls e ACM's First Electronic Pub	may save mo						
ELT					ure Electronic Voting Over the Technology, May 27, 1997		Web,"					

EXAMINER	ĈC	1_	DATE CONSIDERED	
*EXAMINER:		ered, whether or not criteria is	n conformance with MPEP 609. Draw line through citation if not in conformance and not	

					COMPLETE IF KNOWN			
	O P F				Application Number	10/081,863		
		INFORMATION			Confirmation Number	2605		
/		STATEMENT E			Filing Date	February 20, 2002		
_ '	SEP 2 6 2002	방 Form PTO-14			First Named Inventor	C. Andrew Neff		
BET TO	Å	Use several she	ets if necessary)	Group Art Unit	2132		
B	> 2+				Examiner Name	Unknown		
	4 TEMBORAL	1	of	1	Attorney Docket No.	324628006US3		

				·	U.S. PATENT DOCUMENTS		·	
Examiner Initials	Cit	e	S. Patent or Ap	plication Kind Code (if known)	Name of Patentee or Inventor of Cited Document	Date of Publication or Filing Date of Cited Document	Pages, Columns, Line Where Relevant Figures Appear	es,
ECT		5,7	08,714		López et al.	1/13/98	33.33 4	
							-11 /CD	
•						RECE	IVED	
						SEP 3	0 2002	
,						Technology		
·								
,								
	<u></u>							
	1	· · · · · · · · · · · · · · · · · · ·		F	OREIGN PATENT DOCUMENTS		,	
Examiner Initial	Cite No.	For Office	NUMBER	Application Kind Cod (if know	· · · · · · · · · · · · · · · · · ·	Date of Publication or Filing Date of Cited Document	Pages, Columns, Lines, Where Relevant Figures Appear	Т
······ <u>:</u>								+
								_
					ART-NON PATENT LITERATUR			
Examiner Initials	Cite No.	(6	Include nam ook, magazine	e of the auth , journal, ser	or (in CAPITAL LETTERS), title of the ar ial, symposium, catalog, etc.), date, pag and/or country where publish	e(s), volume issue numb	, title of the Item per(s), publisher, city	7
	1							1

EXAMINER	El h	DATE CONSIDERED NOV 'O\							
*EXAMINER:	Initial if reference considered, whether or not criteria is in conform	nance with MPEP 609. Draw line through citation if not in conformance and not							
	considered. Include copy of this form with next communication to application(s).								

PE	•			Patent and Trademark Office: U.S. DEPARTMENT OF COMMER					
200				Co	OMPLETE IF KNOWN				
o 2 Substitute tisto	rm 1449A/PTO			Application Number 10/081,863					
()				Confirmation Number	2605				
, RE / 11	NFORMATION	DISCLOSUR	E	Filing Date	February 20, 2002				
Wa TRANGARE II	TATEMENT B	Y APPLICAN	Т	First Named Inventor	C. Andrew Neff				
				Group Art Unit	2132				
	(use as many she	ets as necessary)		Examiner Name					
Sheet	1	of	2	Attorney Docket No.	324628006US3				

Name of Patente or Applicant Specific Document Name of Patente or Applicant Name of October Name of O						1	U.S. PATENT DOCUMENTS	S			
5,400,248 Chisholm 3/21/95 5,495,532 Kilian et al. 2/27/96 5,521,980 Brands 5/28/96 RECEIVED 5,521,980 Kilian et al. 10/28/97 SEP 2 6 2002 5,717,759 Micali 2/10/98 5,864,667 Barkan 1/26/99 FOREIGN PATENT DOCUMENTS *EXAMINER INITIALS* **EXAMINER No. Office Number (fin Code Number of Chied Document Officied Off	l .			R Kind C				Da:		Where Relevant Passages or	r
S,400,248 Chisholm 3/21/95	E17		5,278,	753		Graf	t, III	1/1	1/94		
5,521,980 Brands 5/28/96 RECEIVED 5,682,430 Kilian et al. 10/28/97 SEP 2 5 2002 5,717,759 Micali 2/10/98 Technology Center 2100 5,864,667 Barkan 1/26/99 Technology Center 2100 5,878,399 Peralto 3/2/99 FOREIGN PATENT DOCUMENTS FOREIGN PATENT DOCUMENTS *EXAMINER Of Particular or Applicant Of Cited Document Number (firstown) ECT EP 0 697 776 A2 NEC Corporation 2/21/96 EP 0 743 620 A2 NEC Corporation 11/20/96 EP 0 743 620 A2 NEC Corporation 11/20/96 WO 98/14921 Certco, LLC 4/9/98 OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS *EXAMINER No. Include name of like author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, or No.	i		5,400,	248		Chis	holm	3/2	1/95		
S,682,430 Kilian et al. 10/28/97 SFP 2 6 2002	·		5,495,	532		Kilia	n et al.	2/2	7/96		
S,717,759 Micali 2/10/98 Technology Center 2100			5,521,	980		Bran	ds	5/2	8/96 RI	ECEIVED	
S,717,759 Micali 2/10/98 Technology Center 2100			5,682,	430		Kilia	n et al.	10	/28/97 SI	P 2 6 2002	
S,864,667 Barkan 1/26/99			5,717,	759		Micali			0/98		
FOREIGN PATENT DOCUMENTS *EXAMINER No. Office Number (if known) ECT EP 0 697 776 A2 NEC Corporation 2/21/96 BP 0 743 620 A2 NEC Corporation 11/20/96 WWO 98/14921 Certco, LLC 4/9/98 *EXAMINER No.			5,864,	667		Bark	an	1/2	6/99	logy center 2100	
EXAMINER INITIALS Cite Number Kind Code Office Number Kind Code (if known)	V	5,878,399 Peralto				lto	3/2	1/99			
EXAMINER INITIALS Cite Number Kind Code Office Number Kind Code (if known)	· · · · · · · · · · · · · · · · · · ·					- FO	DELCAL DATES DA CALDAGE	NIOCO	,		
Name of Patente or Applicant of Cited Document Name of Patente or Applicant Name of Patente or Applicant of Cited Document Name of Patente or Applicant Name of Patente or Applica		r	<u> </u>			FOI	REIGN PATENT DOCUME	NI		Pages Columns Lines Where	ī
ECT EP 0 697 776 A2 NEC Corporation 2/21/96 EP 0 743 620 A2 NEC Corporation 11/20/96 WO 98/14921 Certco, LLC 4/9/98 OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS *EXAMINER Include name of the author (in CAPITAL LETTERS), tille of the article (when appropriate), tille of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published. Benaloh, J., "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag, Berlin, 1987 ECT Benaloh, J., et al., "Distributing the Power of a Government to Enhance the Privacy of Voters", ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986 ECT Benaloh, J., an implementable secure voting scheme", Computers & Security, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338 Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182 Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in				1	Kind C		de of Cited Document			Relevant Passages or Relevant	Т
EP 0 743 620 A2 NEC Corporation 11/20/96 WO 98/14921 Certco, LLC 4/9/98 OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS *EXAMINER Not Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published. ECT Benaloh, J., "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag, Berlin, 1987 Benaloh, J., et al., "Distributing the Power of a Government to Enhance the Privacy of Voters", ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986 ECT Borrell, Joan et al., "An implementable secure voting scheme", Computers & Security, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338 Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182 Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in	FIT				~~~				2/21/96		
OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS *EXAMINER INITIALS* No. Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published. ECT Benaloh, J., "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag, Berlin, 1987 Benaloh, J., et al., "Distributing the Power of a Government to Enhance the Privacy of Voters", ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986 ECT Borrell, Joan et al., "An implementable secure voting scheme", Computers & Security, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338 Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182 Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in	1				+				-		
OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS *EXAMINER INITIALS* No. Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published. ECT Benaloh, J., "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag, Berlin, 1987 Benaloh, J., et al., "Distributing the Power of a Government to Enhance the Privacy of Voters", ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986 Borrell, Joan et al., "An implementable secure voting scheme", Computers & Security, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338 Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182 Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in	1,				+						
EXAMINER INITIALS **O.** **INITIALS* **O.** **Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published. **ECT* **Benaloh, J., "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag, Berlin, 1987 **Benaloh, J., et al., "Distributing the Power of a Government to Enhance the Privacy of Voters", ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986 **ECT* **Benaloh, J., et al., "An implementable secure voting scheme", Computers & Security, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338 **Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182 **Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 **Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in	V .	1						········		*******	J
Journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published. Benaloh, J., "Secret Sharing Homomorphisms: Keeping Shares of a Secret Secret", Advances in Cryptology CRYPTO 1986, Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag, Berlin, 1987 Benaloh, J., et al., "Distributing the Power of a Government to Enhance the Privacy of Voters", ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986 Borrell, Joan et al., "An implementable secure voting scheme", Computers & Security, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338 Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182 Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in	·			OTHER PE	OL	R AR	T-NON PATENT LITERAT	UR	E DOCUMENT	S	
- CRYPTO 1986, Lecture Notes in Computer Science, pp. 251-260, Springer-Verlag, Berlin, 1987 Benaloh, J., et al., "Distributing the Power of a Government to Enhance the Privacy of Voters", ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986 Borrell, Joan et al., "An implementable secure voting scheme", Computers & Security, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338 Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182 Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in											Т
Benaloh, J., et al., "Distributing the Power of a Government to Enhance the Privacy of Voters", ACM Symposium on Principles of Distributed Computing, pp. 52-62, 1986 Borrell, Joan et al., "An implementable secure voting scheme", Computers & Security, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338 Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182 Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in	ECT										
Borrell, Joan et al., "An implementable secure voting scheme", Computers & Security, Elsevier Science, Ltd., Great Britain, 1996, Vol. 15, No. 4, pp. 327-338 Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182 Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in	ELT		Benalo	oh, J., et al.,	"Di	stribut	ing the Power of a Government	t to	Enhance the Priva		
Chaum, D, "Elections with Unconditionally-Secret Ballots and Disruption Equivalent to Breaking RSA", EUROCRYPT 1988, pp. 177-182 Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in	ECT		Borrel	l, Joan et al.,	'An	imple	mentable secure voting scheme", o			Elsevier Science, Ltd.,	
Chaum, D., "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communications of the ACM, 24(2):84-88, 1981 Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in	ELT		Chaun	n, D, "Election	ns v	with U	Inconditionally-Secret Ballots an	d Di	isruption Equivaler	nt to Breaking RSA",	
Cramer, R, et al., "A Secure and Optimally Efficient Multi-Authority Election Scheme", Advances in	FCT		Chaun	n, D., "Untrac	eabl	le Elec		nd D	igital Pseudonyms	", Communications of	
Cryptology - EUROCRYPT 1997, Lecture Notes in Computer Science, Springer-Verlag, 1997.	573		Crame	er, R, et al.,	"A	Secur					

EXAMINER	9 0			DATE CON	SIDERED				
	2 ع	مرك		1	NOV	'05			
				1	1000	$\overline{\mathcal{C}}$			
* ITY A MINICO.	Initial if mafarance	anneidead w	<u> </u>	:a :		600	D C	41	

Initial if reference considered, whether or not criteria is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Append for use through 10/31/99. OMB 0651-0031
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449A/PTO FE JC2 INFORMATION DISCLOSURE TATEMENT BY APPLICANT E (use as many sheets as necessary)				COMPLETE IF KNOWN		
				Application Number	10/081,863	
				Confirmation Number	2605	
				Filing Date	February 20, 2002	
				First Named Inventor	C. Andrew Neff RECEIVED	
				Group Art Unit	2132 IEOLIVED	
				Examiner Name	SEP 2 6 2002	
Sheet	2	of	2	Attorney Docket No.	324628006US3	
ATENT 5	ОТИ	ED DDIOD AD	C NIONI DAT	TENT LITERATURE	DOCUMENTS Technology Center 2100	

		OTHER PRIOR ART-NON PATENT LITERATURE DOCUMENTS			
*EXAMINER INITIALS	Cite No.	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume/issue number(s), publisher, city and/or country where published.			
EG		Cramer, R., et al., "Multi-Authority, Secret-Ballot Elections with Linear Work", Advances in Cryptology – EUROCRYPT 1996, Lecture Notes in Computer Science, Springer-Verlag, Berlin, 1996			
ECT		Cramer, R., et al., "Proofs of Partial Knowledge and Simplified Design of Cryptology - CRYPTO 1994, Lecture Notes in Computer Science, pp. 174-187, Springer-Verlag, Berlin, 1994			
ECT		Cranor, Lorrie et al., "Sensus: A Security-Conscious Electronic Polling System for the Internet", Proceedings of the Hawaii International Conference on System Sciences, IEEE 1997, pp. 561-570			
ECT		Diffic, W., et al., "New Directions in Cryptography", IEEE Transactions on Information Theory, 22(6):644-654, 1976			
ECT		ElGamal, T., "A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", IEEE Transactions on Information Theory, IT-31(4):469-472, 1985			
ELT		Fiat, A., et al., "How to Prove Yourself: Practical Solutions to Identification and Signature Problems", Advances in Cryptology – CRYPTO 1986, Lecture Notes in Computer Science, pp. 186-194, Springer-Verlag, New York, 1987			
ECT		Fujioka, A., et al., "A Practical Secret Voting Scheme for Large Scale Elections", Advances in Cryptology – AUSCRYPT 1992, Lecture Notes in Computer Science, pp. 244-251, Springer-Verlag, 1992			
巨ケ		Gennaro, R., "Achieving independence efficiently and securely", Proceedings 14th ACM Symposium on Principles of Distributed Computing (PODC 1995), New York 1995			
ECT		Iversen, K., "A Cryptographic Scheme for Computerized General Elections", CRYPTO 1991, pp. 405-419			
ECT		Jan, Jin-Ke et al., "A Secure Electronic Voting Protocol with IC Cards", Elsevier Science Inc., New York, J. Systems Software 1997, 39:93-101			
EUT		Mu, Yi et al., "Anonymous Secure E-Voting over a Network", Proceedings, Annual Computer Security Applications Conference, IEEE 1998, pp. 293-299			
ECT		Odlyzko, A. M., "Discrete logarithms in finite fields and their cryptographic significance", Advances in Cryptology – EUROCRYPT 1984, Notes in Computer Science, Springer-Verlag, 1984			
ECT		Park, C., et al., "Efficient Anonymous Channel and All/Nothing Election Scheme", Advances in Cryptology – EUROCRYPT 1993, Lecture Notes in Computer Science, pp. 248-259, Springer-Verlag, 1993			
ELT		Pedersen, T., "A Threshold Cryptosystem without a Trusted Party", Advances in Cryptology – EUROCRYPT 1991, Lecture Notes in Computer Science, pp. 522-526, Springer-Verlag, 1991			
ECT		Sako, K., et al, "Receipt-Free Mix-Type Voting Scheme – A practical solution to the implementation of a voting booth", EUROCRYPT 1995, pp. 393-403			
ECT		Sako, K., et al., "Secure Voting Using Partially Compatible Homomorphisms", Advances in Cryptology – CRYPTO 1994, Lecture Notes in Computer Science, Springer-Verlag, 1994			
ECT	L	Schnorr, C.P., "Efficient Signature Generation by Smart Cards", Journal of Cryptology, 4(3):161-174, 1991			
ECT		Schoenmakers, B., "A Simple Publicly Verifiable Secret Sharing Scheme and its Application to Electronic Voting", Advances in Cryptology - CRYPTO 1999, Lecture Notes in Computer Science, pp. 1-17, Springer-Verlag 1999			
ECT		Shamir, A., "How to Share a Secret", Communications of the ACM, 22(11):612-613, 1979			

EXAMINER	DATE CONSIDERED		
EC 2-	1 NOV '05		
* FXAMINER: Initial if reference considered whether or not criteria	s in conformance with MDED 600. Draw line through situation if not in		